D

Transportation Security Administration

Extension of Agency Information Collection Activity Under OMB Review: Cybersecurity Measures for Surface Modes

AGENCY: Transportation Security Administration, DHS.

ACTION: 30-day Notice.

SUMMARY: This notice announces that the Transportation Security Administration (TSA) has forwarded the Information Collection Request (ICR), Office of Management and Budget (OMB) control number 1652-0074, abstracted below, to OMB for an extension of the currently approved collection under the Paperwork Reduction Act (PRA). The ICR describes the nature of the information collection and its expected burden. Specifically, the collection involves the submission of data concerning the designation of a Cybersecurity Coordinator; the reporting of cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency; the development of a cybersecurity contingency/recovery plan to address cybersecurity gaps; and the completion of a cybersecurity assessment.

DATES: Send your comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. A comment to OMB is most effective if OMB receives it within 30 days of publication.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting "Currently under Review - Open for Public Comments" and by using the find function.

FOR FURTHER INFORMATION CONTACT: Christina A. Walsh, TSA PRA Officer, Information Technology, TSA-11, Transportation Security Administration, 6595

Springfield Center Drive, Springfield, VA 20598-6011; telephone (571) 227-2062; e-mail TSAPRA@tsa.dhs.gov.

SUPPLEMENTARY INFORMATION: TSA published a *Federal Register* notice, with a 60-day comment period soliciting comments, of the following collection of information on November 14, 2022, 87 FR 68185.

Comments Invited

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The ICR documentation will be available at https://www.reginfo.gov upon its submission to OMB. Therefore, in preparation for OMB review and approval of the following information collection, TSA is soliciting comments to—

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Information Collection Requirement

Title: Cybersecurity Measures for Surface Modes.

Type of Request: Extension.

OMB Control Number: 1652-0074.

Form(s): TSA Optional Forms. TSA Surface Cybersecurity Vulnerability Assessment Form.

Affected Public: Owner/Operators with operations identified in 49 CFR part 1580 (Freight Rail), 49 CFR part 1582 (Mass Transit and Passenger Rail), and 49 CFR part 1584 (Over-the-Road Bus).

Abstract: Under the authorities of 49 U.S.C. 114, TSA may take immediate action to impose measures to protect transportation security without providing notice or an opportunity for comment.[1] On December 17, 2021, TSA issued the Security Directive (SD) 1580-21-01 series, *Enhancing Rail Cybersecurity,* and the SD 1582-21-01 series, *Enhancing Public Transportation and Passenger Railroad Cybersecurity,* which remain in effect as revised, mandating TSA-specified Owner/Operators of "higher risk" railroads and rail transit systems, respectively, to implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure; these security directives became effective December 31, 2021. In addition, on October 18, 2022, TSA issued the SD 1580/1582-2022-01 series, *Rail Cybersecurity Mitigation Actions and Testing,* which applies to Owner/Operators of the "Higher Risk" freight railroads identified in 49 CFR 1580.101 and additional TSA-designated freight and passenger railroads. This security directive, which is complementary to the requirements in the previous directives, took effect on October 24, 2022. On October 26, 2022, OMB approved TSA's request for an emergency approval, revising this information collection. *See* ICR Reference Number: 202210-1652-001. The collection covers both mandatory reporting under the security directives and collection of information voluntarily submitted under Information Circular (IC) 2021-01, *Enhancing Surface Transportation Cybersecurity*, which recommended voluntary implementation of actions and reporting by Owner/Operators not covered by

[1] TSA issues security directives for surface transportation operators under the statutory authority of 49 U.S.C. 114(l)(2)(A). This provision, from section 101 of the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71 (115 Stat. 597; Nov. 19, 2001), states: "Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary."

the security directives. The OMB approval allowed for the additional institution of mandatory reporting requirements and collection of information voluntarily submitted. *See* ICR Reference Number: 202111-1652-003. TSA is now seeking renewal of this information collection for the maximum three-year approval period.

The cybersecurity threats to surface transportation infrastructure that necessitate these collections are within TSA's statutory responsibility and authority for "security in all modes of transportation … including security responsibilities … over modes of transportation that are exercised by the Department of Transportation." *See* 49 U.S.C. 114(d).

The requirements in the security directives and the recommendations in the IC allow TSA to execute its security responsibilities within the surface transportation industry, through awareness of potential security incidents and suspicious activities.

A. SD 1580/82-2022-01 Series

This security directive series includes the following information collection:

1. Submission of a Cybersecurity Implementation Plan to TSA for approval that identifies how the Owner/Operator will meet the required security outcomes in the SD;
2. Submission of an Annual Audit Plan for the required Cybersecurity Assessment Program; and
3. Documentation provided to TSA upon request as necessary to establish compliance.

B. SD 1580-21-01, SD 1582-21-01, and IC 2021-01 Series.

These security directives and the IC remain in effect and include the following information collection requirements for the security directives and voluntary collection under the IC:

1. Provide contact information for a designated Cybersecurity Coordinator to TSA.
2. Report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency.
3. Submit a cybersecurity incident response plan to TSA.
4. Complete and submit a cybersecurity vulnerability assessment using a form provided by TSA.

TSA will use the collection of information to ensure compliance with TSA's cybersecurity measures required by the security directives and the recommendations under the IC.

Owner/Operators can complete and submit the required information via email or other electronic options provided by TSA. Documentation of compliance must be provided upon request. As the measures in the IC are voluntary, the IC does not require Owner/Operators to report on their compliance.

Portions of the responses that are deemed Sensitive Security Information (SSI) are protected in accordance with procedures meeting the transmission, handling, and storage requirements of SSI set forth in 49 CFR part 1520.[2]

Number of Respondents: 781.

Estimated Annual Burden Hours: An estimated 96,163 hours annually.

Dated: March 6, 2023.

[2] In addition, all data in TSA systems are statutorily required to comply with the Federal Information Security Modernization Act 2014 (FISMA) following the National Institute of Standards and Technology Special Publication 800.37 REV2 or Risk Management Framework, and other federal information security requirements including Federal Information Processing Standards 199 and Executive Order 14028. All systems, networks, servers, clouds and endpoints under the FISMA boundary are hardened to meet the Department of Defense Security Technical Implementation Guidelines, as well as DHS Policy (4300.A) and TSA policy (TSA IA Handbook).

Christina A. Walsh,

TSA Paperwork Reduction Act Officer,

Information Technology.

[FR Doc. 2023-04859 Filed: 3/8/2023 8:45 am; Publication Date: 3/9/2023]